Capítulo 5
Implementación, Administración y Monitoreo de Group Policy

Durante este capítulo Usted irá asimilando los conocimientos que necesita para hacer una correcta administración, diseño e implementación de Group Policy.

Para poder realizar las prácticas de esta unidad es necesario que haya concluido las prácticas de los capítulos 2 y 3.

1. Introducción

Usted utiliza Group Policy en Active Directory® para centralizar el manejo de usuarios y computadoras en una empresa. Configurando Group Policy puede centralizar policies para una organización entera, dominio, sitio u organizational unit, y asimismo puede descentralizar la configuración de Group Policy, configurándolo para cada departamento en el nivel organizational unit.

Usted puede asegurarse que los usuarios tengan los ambientes que requieren para realizar sus trabajos y hacer cumplir las políticas de las organizaciones, incluyendo reglas de negocio, metas y requisitos de seguridad. Además, puede bajar el Total Cost of Ownership controlando ambientes del usuario y de computadora, de modo tal que se reduzca el nivel de ayuda técnica a los usuarios y la productividad perdida de los mismos a causa de sus errores.

Al terminar este capítulo Usted podrá:

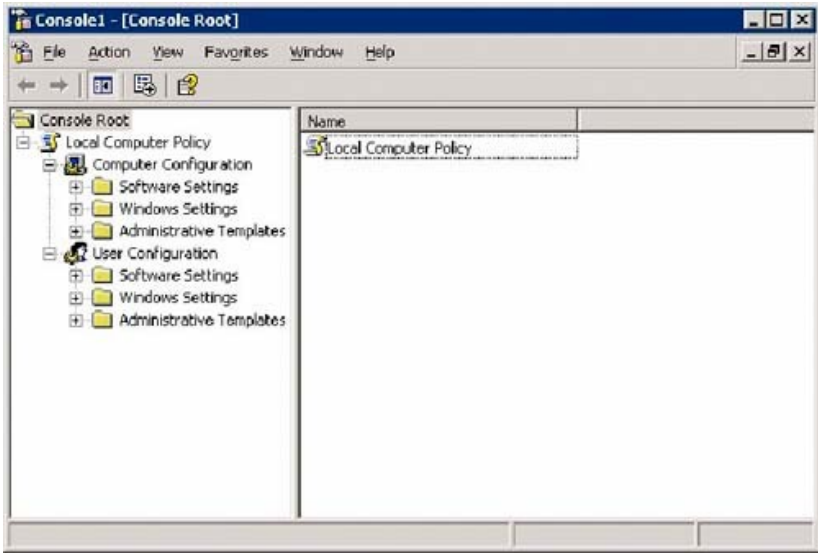
- Crear y configurar Group Policy objects (GPOs).
- Configurar intervalos de actualización de Group Policy y configuraciones de Group Policy.
- Administrar GPOs.

1.1. ¿Qué es Group Policy?

Group Policy le otorga control de administración sobre los usuarios y las computadoras de su red, y por lo tanto le permite definir el estado del ambiente de trabajo de los usuarios una sola vez, confiando en Microsoft® Windows® Server 2003 para hacer cumplir continuamente la configuración de Group Policy que definió. También podrá aplicar configuraciones de Group Policy a través de una organización entera o a grupos específicos de usuarios y de computadoras.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by ITsitio



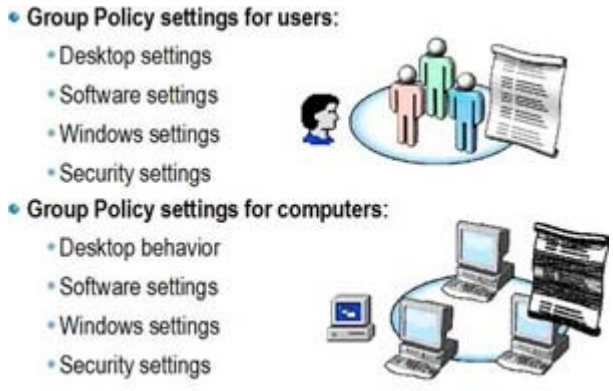
Para más información acerca de Group Policy:

Microsoft IntelliMirror®.

Group Policy Settings Overview.

1.2. ¿Qué son User y Computer Configuration Settings?

Usted puede hacer cumplir los Group Policy Settings para las computadoras y los usuarios usando Computer Configuration y User Configuration en Group Policy.



Group Policy Settings para usuarios incluye configuraciones específicas del sistema operativo, configuraciones de escritorio, configuraciones de seguridad, opciones de aplicaciones assigned y published, configuraciones de aplicaciones, opciones de folder redirection, y scripts de user logon y logoff. Los Group Policy Settings de usuario se aplican cuando los usuarios inician sesión en la computadora y durante un ciclo de actualización periódico.

Group Policy Settings modifica el ambiente de escritorio del usuario para los requisitos particulares o hace cumplir lockdown policies en usuarios, y está contenido debajo de ***User Configuration*** en el editor de Group Policy Object.

Debajo de User Confiugration, también se encuentran:

- La carpeta Software Settings: contiene configuraciones de software que se aplican a los usuarios sin importar en qué computadora inicien sesión. Esta carpeta también contiene configuraciones que se coloquen allí de Independent Software Vendors (ISVs).

- La carpeta Windows Settings: contiene configuración Windows que se aplica a los usuarios sin importar en qué computadora inicien sesión. Esta carpeta también contiene los siguientes puntos: **Folder Redirection, Security Settings y Scripts**.

Group Policy Settings para las computadoras incluye la manera en que el sistema operativo se comporta, el comportamiento de escritorio, configuraciones de seguridad, scripts de startup y shutdown, opciones de aplicaciones assigned a la computadora y configuraciones de aplicaciones. Las Group Policy relacionadas a la computadora, se aplican cuando el sistema operativo se inicializa y durante un ciclo periódico de

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

actualización. En general, las configuraciones de computadora Group Policy toman precedencia al estar en conflicto con Group Policy de usuario.

Las Group Policy Settings que modifican el ambiente para requisitos particulares de escritorio y para todos los usuarios de una computadora, o que hacen cumplir las políticas de seguridad en las computadoras de una red, se contienen debajo de ***Computer Configuration*** en el editor de Group Policy Object.

Debajo de Computer Configuration, también se encuentran:

- La carpeta Software Settings: contiene las configuraciones de software que se aplican a todos los usuarios que inicien sesión en la computadora. Esta carpeta posee configuración de instalación de software y puede contener otras configuraciones que se coloquen allí de ISVs.

- La carpeta Windows Settings: contiene configuraciones Windows que se aplican a todos los usuarios que inicien sesión en la computadora. Esta carpeta también contiene los siguientes puntos: **Security Settings y Scripts**.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Security Settings está disponible debajo de la carpeta Windows Settings que se encuentra debajo de Computer Configuration y User Configuration en el editor de Group Policy Object. Security Settings o Security Policies son las reglas que Usted configura en una computadora o las computadoras múltiples que protegen recursos en una computadora o una red. Con Security Settings, Usted puede especificar Security Policy de una organizational unit, domain o site.

Para más información sobre extender Group Policy, ver los métodos Avanzados extendiendo Group Policy en:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SPconcepts_30.asp

1.3. Práctica 1: Configurando Local Computer Policy Settings

Para agregar Group Policy Object Editor a una CustomMMC deberá:

1. Abrir una CustomMMC.
2. Agregar el snap-in Group Policy Object Editor.
3. Guardar la CustomMMC.

Para evitar que los usuarios apaguen el servidor usando Local Policy Setting deberá:

1. Expandir, en la CustomMMC, el snap-in ***Local Computer Policy***.
2. Expandir, en la consola, ***User Configuration***. Expandir ***Administrative Templates*** y después hacer click en S***tart Menu and Taskbar***.
3. Hacer doble-click en ***Remove and prevent access to the Shut Down command***, del panel de los detalles
4. Hacer click en ***Enabled*** del cuadro ***Remove and prevent access to the Shut Down command Properties***, y después hacer click en ***OK***.
5. Cerrar y guardar todos los programas y hacer log off.

Para probar la policy deberá:

1. Iniciar sesión como ***User*** con una contraseña.
2. Hacer Click en ***Start*** y verificar que el botón ***Shut Down*** se haya quitado del menú ***Start***.
3. Cerrar y guardar todos los programas y hacer log off.

1.4. Las herramientas usadas para crear GPOs

- ***Active Directory Users and Computers***

Usted puede abrir el editor de Group Policy Object desde Active Directory Users and Computers para administrar GPOs para dominios y organizational units. En el cuadro Properties para un dominio u organizational unit, hay una lengüeta Group Policy, con la cual se puede manejar GPOs para el dominio u organizational units.

- ***Active Directory Sites and Services***

Usted puede abrir el editor de Group Policy Object desde Active Directory Sites and Services para manejar GPOs de sites. En el cuadro Properties para el site, hay una lengüeta Group Policy, con la cual se puede manejar GPOs para el site.

- ***Group Policy Management Console***

La Group Policy Management Console es un sistema de interfases programables para el manejo de Group Policy, así como las MMC snap-in que se construyen en estas interfases programables también. Los componentes de Group Policy Management, por su parte, consolidan la administración de Group Policy a través de la empresa.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

La Group Policy Management Console combina la funcionalidad de componentes múltiples en una sola interfaz de usuario (UI). La UI se estructura para emparejar la manera en que se utiliza y maneja Group Policy. Asimismo incorpora la funcionalidad relacionada con Group Policy de las herramientas siguientes en una sola MMC snap-in:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Resultant Set of Policy (RSoP)

Group Policy Management también proporciona las siguientes capacidades extendidas que no estaban disponibles en herramientas anteriores de Group Policy. Con Group Policy Management, Usted puede:

Hacer Back up y restore de GPOs.

- Copiar e importar GPOs.
- Usar filtros Windows Management Instrumentation (WMI).
- Generar reportes de GPO y RSoP.
- Búscar para GPOs.

- new! ***Group Policy Management vs. default Group Policy tools***

Antes de Group Policy Management, Usted administraba Group Policy usando una variedad de herramientas Windows, incluyendo Active Directory Users and
Computers, Active Directory Sites and Services y RSoP. Pero ahora, Group Policy Management consolida la administración de todas las tareas base de Group Policy en una sola herramienta. Gracias a esta administración consolidada, la funcionalidad de Group Policy ya no es requerida en las otras herramientas.

Después de instalar Group Policy Management, Usted aún utiliza cada una de las herramientas de Active Directory para sus propósitos previstos de administración de directorio, por ejemplo, crear un usuario, computadora y grupo. Sin embargo, usted puede utilizar Group Policy Management para realizar todas las tareas relacionadas con Group Policy. La funcionalidad de Group Policy ya no estará disponible con las herramientas de Active Directory cuando instale Group Policy Management.

Group Policy Management no sustituye al editor de Group Policy Object. Usted todavía debe editar GPOs, usando el editor de Group Policy Object. Group Policy Management integra la funcionalidad de edición proporcionando acceso directo al editor de Group Policy Object.

Nota: La Group Policy Management Console no viene con Windows Server 2003.

Usted debe descargarlo de:

http://www.microsoft.com/downloads/details.aspx?FamilyId=F39E9D60-7E41-4947-82F5-3330F37ADFEB&displaylang=en

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

1.5. Práctica 2: ¿Cómo crear una GPO?

Utilice los procedimientos siguientes para crear un nuevo GPO o un link a una GPO existente, usando Active Directory Users and Computers, y para crear una GPO en un site, dominio u organizational unit.

Para crear una GPO nueva o hacer un link a una GPO existente usando Active Directory Users and Computers:

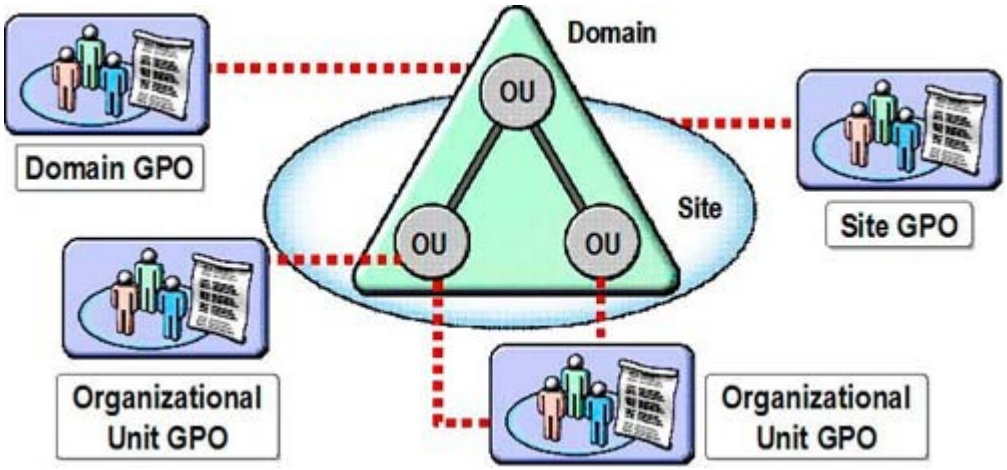
1. Hacer click derecho en el ***contenedor de Active Directory*** (dominio u organizational unit), que está en el Active Directory Users and Computers, para crear una GPO. Después hacer click en ***Properties***.
2. Elegir una de las opciones siguientes, en el cuadro ***Properties***, sobre la lengüeta ***Group Policy***:

   - ***Para crear una GPO nueva***, hacer click en New, ingresar un nombre para la GPO nueva y presionar ENTER.

   - ***Para hacer un link a una GPO existente***, hacer click en Add y seleccionar la GPO de la lista.

La GPO o el link que usted crea, se exhibe en la lista de GPOs que están linkeadas al contenedor de Active Directory.

1.6. ¿Qué es un GPO Link?



Todas las GPOs se almacenan en un contenedor de Active Directory llamado Group Policy Objects. Cuando una GPO es utilizada por un site, dominio u organizational unit, la GPO es linkeada al contenedor Group Policy Objects. Consecuentemente, Usted puede centralizar la administración y el deploy de GPOs a muchos dominios u organizational units.

Cuando Usted crea un GPO link a un site, dominio u organizational unit, podrá realizar dos operaciones separadas: crear la GPO nueva y linkearla al site, dominio u organizational unit. Al delegar permisos para linkear una GPO al dominio, organizational unit o site, Usted tendrá que modificar los permisos para el dominio, organizational unit o site que desee delegar.

Por defecto, solamente miembros de los grupos Domain Admins y Enterprise Admins tienen los permisos necesarios para linkear GPOs a domains y organizational units. Únicamente los miembros del grupo Enterprise Admins tienen los permisos para linkear GPOs a sites. Miembros del grupo Group Policy Creator Owners pueden crear GPOs, pero no pueden linkear.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

Cuando Usted crea una GPO en el contenedor Group Policy Objects, la GPO no se aplica a ningún usuario o computadora hasta que el GPO link sea creado. Usted puede crear una unlinked GPO usando Group Policy Management y también puede llegar a crear unlinked GPOs en una organización grande, donde un grupo cree GPOs y otro grupo cree links de GPOs al site, dominio u organizational unit.

1.7. Práctica 3: ¿Cómo crear un GPO Link?

Para realizar esta práctica deberá instalar previamente GPMC. (Vea el punto 4.3 más adelante) Utilice los procedimientos siguientes para crear y linkear GPOs.

- Para linkear una GPO cuando usted lo crea:

1. En la Group Policy Management de la consola, expandir el forest conteniendo el dominio en el cual Usted desea crear y linkear la GPO. Expandir ***Domains*** y realizar uno de los siguientes pasos:

- ***Para crear una GPO y linkearla al dominio***, hacer click derecho en el dominio y después hacer click en Create and Link a GPO Here.

- ***Para crear una GPO y linkearla a una organizational unit***, expandir el dominio que contiene la organizational unit, hacer click derecho en la organizational unit, y después hacer click en ***Create and Link a GPO Here***.

2. En el cuadro ***New GPO***, ingresar el nombre para la GPO nueva y después hacer click en ***OK***.

- Para linkear una GPO existente al site, dominio u organizational unit:

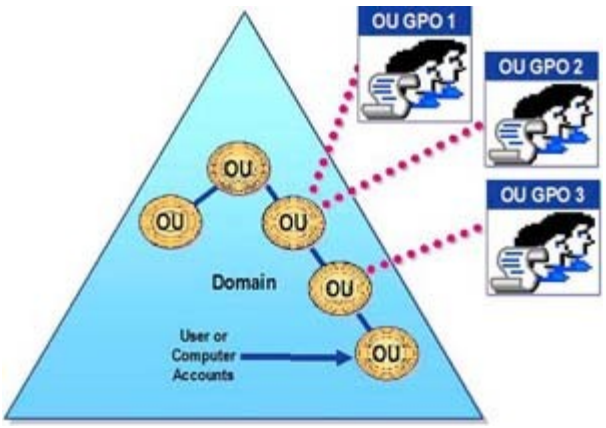
1. En Group Policy Management de la consola, expandir el forest conteniendo el dominio en el cual Usted desea linkear una GPO existente. Expandir ***Domains*** y el dominio.
2. Hacer click derecho en el dominio, site u organizational unit. Después hacer click en ***Link an Existing GPO***.
3. En el cuadro ***Select GPO***, hacer click en la GPO que Usted desea linkear y después hacer click en ***OK***.

1.8. ¿Cómo se heredan permisos de Group Policy en Active Directory?

La orden en la cual Windows Server 2003 aplica GPOs depende del contenedor de Active Directory al cual es linkeada la GPO. Las GPOs se aplican primero al site, después a dominios y por último a organizational units en los dominios.

Un contenedor child hereda GPOs del contenedor parent. Esto significa que un contenedor child puede tener muchos Group Policy Settings aplicados a sus usuarios y computadoras, sin tener un GPO linkeado a él. Sin embargo, no hay jerarquía de dominios como en las organizational units, por ejemplo, las parent organizational units y child organizational units.

Las GPOs son acumulativas, implicando que están heredadas. La herencia de Group Policy es el orden en el cual Windows Server 2003 aplica GPOs. Este orden y la herencia de GPOs determinan, en última instancia, qué configuraciones afectan a usuarios y computadoras. Si hay GPOs múltiples que se fijan en el mismo valor, por defecto la GPO que se aplicó última, tomará precedencia.



Usted puede también tener GPOs múltiples linkeadas al los mismos contenedores. Por ejemplo, puede tener tres GPOs linkeadas a un solo dominio. El orden en el cual se aplican las GPOs puede afectar el resultado de

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

la configuración de Group Policy. Hay también un orden o prioridad de Group Policy y de GPOs para cada contenedor.

1.9. ¿Qué sucede cuando hay conflicto de GPOs?

Las combinaciones complejas de GPOs pueden crear conflictos y consecuentemente requerir modificar el comportamiento de la herencia por defecto. Cuando una configuración de Group Policy se configura para una organizational unit parent y la misma configuración de Group Policy no se configura para la organizational unit child, los objetos de esta última heredan la configuración de Group Policy de la organizational unit parent.

Cuando se configura una Group Policy para ambas, organizacional unit parent y organizational units child, las configuraciones para estas organizational units se aplican. Si las configuraciones son incompatibles, la organizational unit child conserva sus propia configuración de Group Policy. Por ejemplo, una configuración de Group Policy para la organizational unit se aplica por último a la computadora o el usuario sobreescribe la que está en conflicto de configuración de Group Policy para un contenedor, que es de más alta jerarquía en Active Directory.

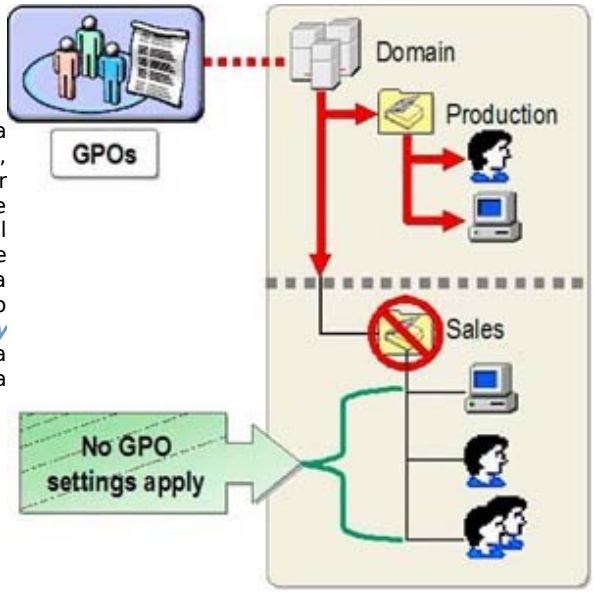
Si el orden de herencia por defecto no resuelve las necesidades de su organización, Usted puede modificar las reglas de herencia para GPOs específicas. Windows Server 2003 proporciona las dos siguientes opciones para cambiar el orden de herencia por defecto:

- ***No Override***
  Esta opción se utiliza para prevenir que contenedores child eliminen una GPO con prioridad más alta de configuración. Esta alternativa es útil para hacer cumplir GPOs que representen reglas de negocio de la organización. La opción ***No Override*** se fija sobre una base individual de GPO. Usted puede fijar esta opción en una o más GPOs según lo requiera. Cuando se fija más de una GPO en ***No Override***, la GPO más alta en la jerarquía de Active Directory, fijada en ***No Override***, tomará precedencia.

- ***Block Policy inheritance***
  Esta opción se utiliza en contenedores child para bloquear herencia de todos los contenedores parent. Es útil cuando una organizational unit requiere una única configuración de Group Policy. ***Block Policy inheritance*** se fija basándose en el contenedor. En caso de conflicto, la opción ***No Override*** toma siempre precedencia sobre la opción ***Block Policy inheritance***.

1.10. Bloqueo de Deployment de GPO

Usted puede prevenir en un contenedor child la herencia de cualquier GPO de los contenedores parent, habilitando ***Block Policy inheritance*** en el contenedor child. De esta manera, evita que el contenedor herede todas las configuraciones Group Policy. Esto es útil cuando un contenedor de Active Directory requiere configuraciones únicas de Group Policy y Usted desea asegurarse que las configuraciones de Group Policy no se hereden. Por ejemplo, se puede utilizar ***Block Policy inheritance*** cuando el administrador de una organizational unit deba controlar todas las GPOs para ese container.



© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

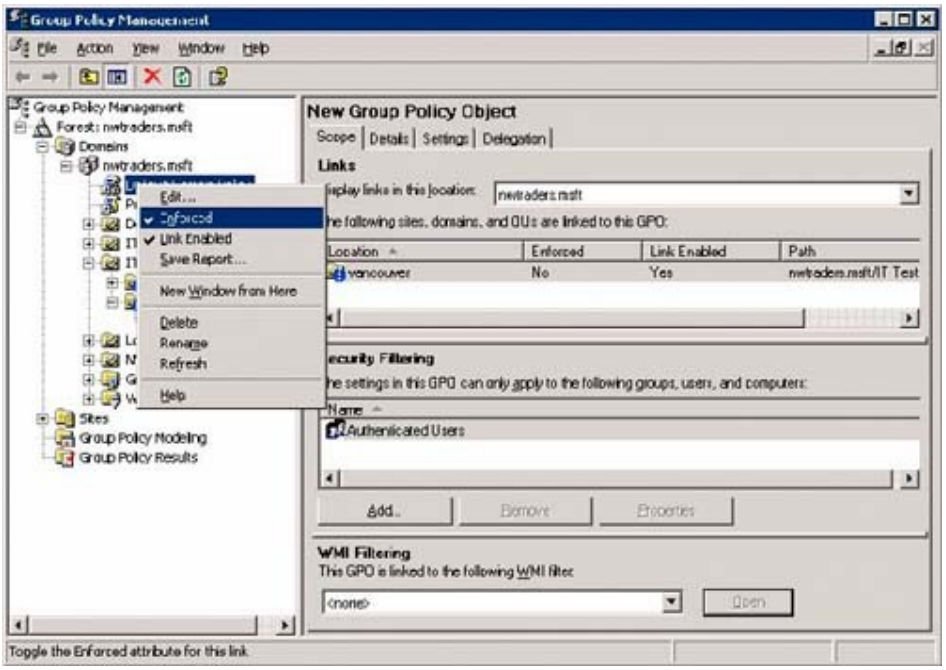
Powered by

Al usar Block Policy inheritance***, deberá considerar lo siguiente:***

- No se puede elegir selectivamente qué GPOs bloquea. ***Block Policy inheritance*** afecta todas las GPOs de todos los contenedores parent, excepto las GPOs configuradas con la opción ***No Override*** sin GPMC instalada y ***Enforced*** con GPMC instalada.

- ***Block Policy inheritance*** no bloquea la herencia de una GPO linkeada a un contenedor parent, si el link se configura con la opción ***No Override***.

1.11. ¿Cómo configurar Group Policy Enforcement?



Importante: Antes de instalar Group Policy Management, la opción ***Enforced*** se llama No Override en Active Directory Users and Computers.

Para configurar enforcement de GPO link deberá:

1. En Group Policy Management de la consola, expandir el forest con el link en el cual Usted desea configurar el enforcement. Luego, seguir uno de siguientes pasos:

   - ***Para configurar enforcement de GPO link a un dominio***, expandir Domains y el dominio que contiene el GPO link.

   - ***Para configurar enforcement de GPO link a una organizational unit***, expandir Domains y el dominio que contiene la organizational unit. Después expandir la organizational unit que pueda incluir parent o child organizational unit y que contenga el GPO link.

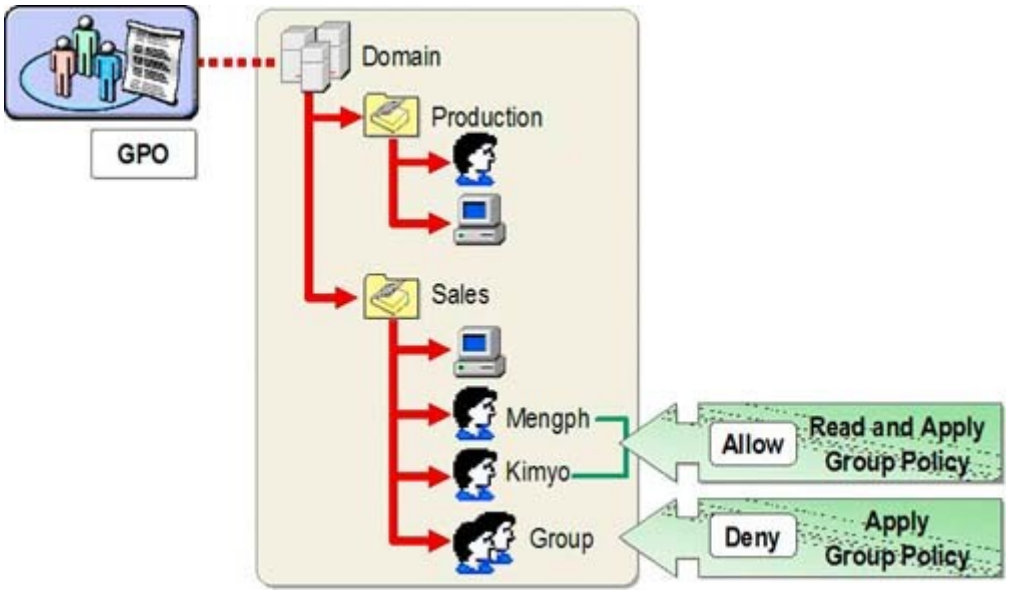
   - ***Para configurar enforcement de GPO link a un site***, expandir Sites, y luego expandir el site que contiene el GPO link.

2. Hacer click derecho en el GPO link y después hacer click en ***Enforced*** para permitir o inhabilitar el enforcement.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

1.12. Filtrado de Deployment de GPO



Por defecto, todos los Group Policy Settings contenidos en las GPOs, afectan al contenedor y se aplican a todos los usuarios y computadoras de ese contenedor, el cual no puede producir los resultados que Usted desea. Usando la característica de filtrado, se puede determinar qué configuraciones se aplican a los usuarios y a las computadoras en el contenedor específico.

Usted puede filtrar el deployment de GPO fijando permisos en el GPO Link para determinar el acceso de lectura o negar el permiso en la GPO. Para que los Group Policy Settings se apliquen a una cuenta de usuario o de computadora, la cuenta debe tener por lo menos el permiso de lectura para una GPO. Los permisos por defecto para una GPO nueva tienen el siguiente Access Control Entries (ACEs):

- Authenticated Users. Permitir read y permitir apply Group Policy
- Domain Admins, Enterprise Admins and SYSTEM. Permitir read, Permitir Write, Permitir Create All Child objects, Permitir Delete All Child objects

Usted puede utilizar los siguientes métodos de filtrado:

- ***Explicitly deny***
  Este método se utiliza al negar el acceso a la Group Policy. Por ejemplo, Usted podría negar explícitamente el permiso al grupo de seguridad de los administradores, lo cual prevendría a los administradores en la organizational unit de la recepción de GPO Settings.
- ***Remove Authenticated Users***
  Usted puede omitir a los administradores de la organizational unit del grupo de seguridad, lo cual significa que no tienen ningún permiso explícito para la GPO.

Para más información acerca de Group Policy:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324743

http://microsoft.com/downloads/details.aspx?FamilyId=D26E88BC-D445-4E8F-AA4E-B9C27061F7CA&displaylang=en

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/management/gp/default.asp

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2. Administración del entorno de usuario

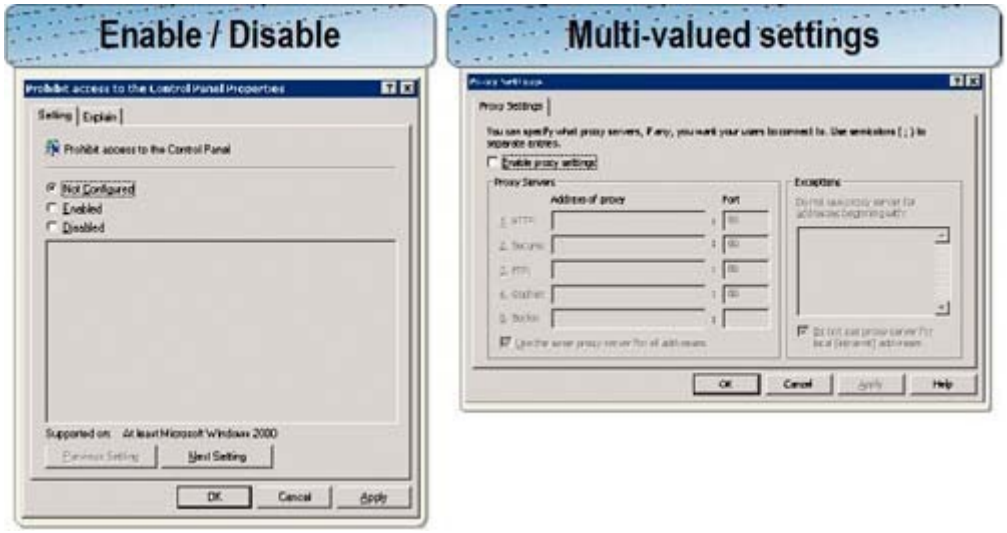
La administración del entorno de usuario implica controlar lo que éstos pueden hacer cuando inician sesión en la red. Esto se hace a través de Group Policy, controlando las computadoras de escritorio, las conexiones de red y las interfaces de usuario. Usted maneja los ambientes de usuario para asegurarse que los mismos tengan lo necesario para realizar sus trabajos. De esta manera, no podrán corromper o configurar incorrectamente sus ambientes.

Cuando Usted configura y maneja ambientes de usuario de forma centralizada, puede realizar las siguientes tareas:

- ***Manejar los usuarios y las computadoras.*** Esto es posible controlando la configuración de escritorio del usuario con policies basadas en registry. Así, Usted se asegura que los usuarios tengan los mismos ambientes, incluso si ellos inician sesión de diversas computadoras. Asimismo, Usted puede controlar cómo Microsoft Windows® Server 2003 maneja el user profiles, el cual conoce la forma en que los datos personales de un usuario están disponibles. Con redirecting user folders de los discos duros locales del usuario a una localización central en un servidor, Usted puede asegurarse que los datos del usuario estén disponibles para ellos, sin importar la computadora desde la cual inicien sesión.

- ***Deploy software.*** El software se instala en las computadoras o en los usuarios con servicio de directorio Active Directory®. Con la instalación del software, Usted puede asegurarse que los usuarios tengan sus programas requeridos, service packs, y hotfixes.

2.1. ¿Qué son los Group Policy Settings Enable o Disable?



Si Usted inhabilita un policy setting, está inhabilitando la acción del policy setting. Por ejemplo, los usuarios por defecto pueden tener acceso al Control Panel. Para ello, Usted no necesita inhabilitar el policy setting ***Prohibit access to the Control Panel***, a menos que previamente haya aplicado un policy setting habilitándolo. En esta situación, Usted habrá fijado otro policy setting para deshabilitar el aplicado previamente.

Esto es provechoso cuando se heredan policy settings y no se desea usar filtrado para aplicar policy settings a un grupo y a otro no. Usted puede aplicar una GPO que permita un policy setting en la parent organizational unit y otro policy setting que deshabilite la GPO en la child organizational unit.

Si Usted permite un policy setting, estará consintiendo la acción del policy setting. Por ejemplo, para revocar a alguien acceso al Control Panel, Usted puede permitir el policy setting ***Prohibit access to the Control Panel***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Un GPO lleva a cabo los valores que cambian registry para los usuarios y las computadoras que están conformes al GPO. La configuración por defecto para un policy setting es ***Not Configured***. Si Usted desea fijar a una computadora o a un usuario un policy setting, de nuevo al valor prefijado o de nuevo a la local policy, deberá seleccionar la opción ***Not Configured***. Por ejemplo, Usted puede permitir un policy setting para algunos clientes, y al usar la opción Not Configured, la policy invertirá a la policy por defecto, o local policy setting.

Algunas GPOs requieren proporcionar una cierta información adicional después de permitir el objeto. Ciertas veces Usted puede necesitar seleccionar un grupo o una computadora si el policy setting necesita volver a dirigir al usuario a una cierta información. Otras veces, para permitir proxy settings, Usted deberá proporcionar el nombre o la dirección Internet Protocol (IP) del proxy server y el número de puerto. Si el policy setting es multi-valued y los settings están en conflicto con otro policy setting, el conflicto de multi-valued settings se substituyen por el último policy setting que fue aplicado.

2.2. Práctica 4: ¿Cómo editar un Group Policy Setting?

Como administrador de sistemas, Usted debe editar Group Policy settings. Utilice el siguiente procedimiento para realizar esta tarea.

1. En Group Policy Management de la consola, navegar los ***Group Policy Objects***.
2. Hacer click derecho en la GPO y después en ***Edit***.
3. En el editor de Group Policy Object, buscar el Group Policy setting que se desear editar, y después hacer doble-click.
4. En el cuadro ***Properties***, configurar el Group Policy setting y después hacer click en ***OK***.

2.3. ¿Qué son los scripts de Group Policy Settings?

Usted puede utilizar los scripts de Group Policy para configurar scripts centralizados que corran automáticamente cuando la computadora se inicia y se apaga, y también cuando los usuarios inician sesión y la cierran. Usted puede especificar cualquier script que corra en Windows Server 2003, incluyendo archivos batch, programas ejecutables y scripts soportados por Windows Script Host (WSH).

Para ayudar al usuario a manejar y configurar sus ambientes, deberá:

- Correr scripts que realicen las tareas que Usted no puede realizar con otros Group Policy settings. Por ejemplo, configurar el entorno de usuario con conexiones de red, conexiones de impresora, shortcuts a aplicaciones y documentos corporativos.

- Limpiar los escritorios cuando los usuarios cierran la sesión y apagan la computadora. Usted puede quitar las conexiones que agregó con los scripts de logon o startup, de modo que la computadora esté en el mismo estado que cuando el usuario la encendió.

- Correr scripts pre-existentes, fijados para manejar los ambientes de usuario hasta que se configure con otro Group Policy settings que remplace esos scripts

Nota: Desde Active Directory Users and Computers, Usted puede asignar scripts de logon individualmente a las cuentas del usuario en el cuadro ***Properties*** de cada uno de ellos. Sin embargo, Group Policy es el método preferido para correr scripts porque se pueden manejar estos scripts centralizados junto con startup, shutdown,
y logoff scripts.

Para más información acerca de scripting, vea TechNet Script Center en:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.4. Práctica 5: ¿Cómo asignar Scripts con Group Policy?

Para implementar script Usted utiliza Group Policy, agregándolo a la configuración apropiada en un Group Policy template. Esto indica que el script puede correr durante el startup, shutdown, logon o logoff.

Para agregar un script a la GPO deberá:

1. En Group Policy Management, editar la GPO.
2. En el editor de Group Policy Object de la consola, buscar User Configuration/Windows Settings/Scripts (Logon/Logoff).
3. En el panel de detalles, hacer doble-click en ***Logon***.
4. En el cuadro ***Logon Properties***, hacer click en ***Add***.
5. En el cuadro ***Add a Script***, configurar cualquiera de las configuraciones siguientes que se desee utilizar. Después, hacer click en ***OK***:
   - ***Script Name.*** Ingresar el path del script o hacer click en ***Browse*** para localizar el archivo de script en la carpeta compartida Netlogon del Domain controller.
   - ***Script Parameters.*** Ingresar los parámetros que se desean utilizar, de la misma manera que se ingresaría en command line.
6. En el cuadro ***Logon Properties***, configurar cualquiera de las siguientes configuraciones que se deseen utilizar:
   - ***Logon Scripts for.*** Esta lista enumera todas los scripts que están actualmente asignados a la GPO seleccionada. Si se asignan múltiples scripts, éstos serán procesados en el orden que se especificó. Para mover el script en la lista, hacer click en el script y después ***Up*** o ***Down***.

2.5. ¿Qué es Folder Redirection?

Cuando Usted redirecciona folders, cambia la locación de las carpetas del disco duro local de la computadora del usuario, a una carpeta compartida en un servidor de la red. Después de redireccionar una carpeta a un servidor, ésta seguirá apareciendo como local para el usuario. Cuatro son las carpetas que forman parte del user profile y que se pueden redireccionar: My Documents, Application Data, Desktop y Start Menu.

Almacenando datos en la red, los beneficios de los usuarios son la disponibilidad creciente y los backup frecuentes de sus datos. Redireccionar carpetas tiene los siguientes beneficios:

- Los datos en las carpetas están disponibles para el usuario, sin importar la computadora cliente desde la que el usuario inicie sesión.
- Los datos en las carpetas se almacenan centralizados, y por esto es más fácil la administración y el backup para su resguardo.
- Los archivos que se localizan adentro de carpetas redireccionadas, como los archivos de un roaming user profile, no se copian y no se guardan en la computadora del usuario que inicia sesión. Esto significa que cuando el usuario inicia sesión en la computadora cliente, no se utilizará espacio de almacenamiento para esos archivos y los datos que puedan ser confidenciales no quedan en dicha computadora.
- Los datos se almacenan en una carpeta compartida de red que puede ser parte de las áreas rutinarias de backup. Esto es más seguro porque no requiere ninguna acción de parte del usuario.
- Como administrador, Usted puede utilizar Group Policy para configurar disk quotas, limitando la cantidad de espacio que es tomado por los usuarios.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.6. Carpetas que pueden ser redireccionadas

Usted puede redireccionar las carpetas My Documents, Application Data, Desktop y Start Menu. Una organización debe redireccionar estas carpetas para preservar datos y configuraciones importantes del usuario. Hay varias ventajas al redireccionar cada una de estas carpetas, que varían según las necesidades de la organización.

Usted puede utilizar redirección para cualquiera de las siguientes carpetas en el user profile:

My Documents
La redirección de My Documents es particularmente ventajosa porque la carpeta tiende a realizarla en un plazo grande.
La tecnología Offline Files da el acceso a usuarios a My Documents, incluso cuando los usuarios no están conectados a la red. Esto es particularmente útil para gente que utiliza las computadoras portátiles.

Application Data
Los Group Policy setting controlan el comportamiento de los Application Data cuando el caching del lado del cliente está habilitado. Esta configuración sincroniza los datos de aplicaciones centralizados en un servidor de la red con la computadora local. Consecuentemente, el usuario puede trabajar en línea o fuera de línea. Si algunos cambios se realizan a los datos de aplicación, la sincronización actualiza los datos del aplicativo sobre el cliente y el servidor.

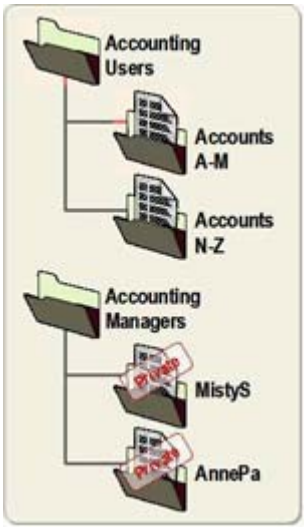
Desktop
Usted puede redireccionar el escritorio y todos los archivos, shortcuts y carpetas a un servidor centralizado.

Start Menu
Cuando se redirecciona el Start Menu, sus subfolders también se redireccionan.

2.7. Configuraciones requeridas para configurar Folder Redirection

Hay tres configuraciones disponibles para Folder Redirection: none, basic y advanced. Basic Folder Redirection es para los usuarios que deben redirigir sus carpetas a un área común o para los usuarios que necesitan que sus datos sean privados.

Usted tiene las siguientes opciones básicas para Folder Redirection:



- ***Redirect folder to the following location***
  Todos los usuarios redireccionan sus carpetas a un área común donde pueden ver o utilizar otros datos en carpetas redirecionadas. Para hacer esto, elija la configuración ***Basic*** y configure la ***Target folder location to Redirect folder to the following location.*** Es aconsejable utilizar esta opción para todas las carpetas que contengan los datos que no son privados.

- ***Create a folder for each user under the root path***
  Para los usuarios que necesitan sus carpetas redireccionadas con datos privados, elija configuración ***Basic*** y configure ***Target folder location to Create a folder for each user under the root path.*** Es aconsejable utilizar esta opción para los usuarios que necesitan sus datos privados, como los gerentes que guardan datos personales sobre empleados.

Cuando Usted selecciona ***Advanced . specify locations for various user groups***,
las carpetas son redireccionadas a diferentes locaciones, basadas en grupos de seguridad de los usuarios.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

Las opciones avanzadas para Folder Redirection son las siguientes:

Select a group(s). Aquí es donde se especifica a quién aplicar la redirección.
Target Folder Location. Aquí se pueden elegir cualquiera de las siguientes opciones:

- ***Create a folder for each user under the root path.*** Utilizar para los datos confidenciales.
- ***Redirect to the following location.*** Utilizar para los datos compartidos.
- ***Redirect to the local userprofile location.*** Utilizar para los usuarios que utilizan una mezcla de computadoras cliente que no son parte de Active Directory por un lado y sí lo son por otro.

Root Path. En este cuadro, se especifica el servidor y el nombre de la carpeta compartida a la que se desear redireccionar.

2.8. Práctica 6: ¿Cómo configurar Folder Redirection?

Usted configura Folder Redirection usando el editor de Group Policy Object.

Para configurar Folder Redirection deberá:

1. En Group Policy Management, editar o crear la GPO.
2. En el editor de Group Policy Object de la consola, expandir ***User Configuration***, expandir ***Windows Settings***, y después expandir ***Folder Redirection***. Los íconos para las cuatro carpetas que pueden ser redireccionadas se muestran.
3. Hacer click derecho en la carpeta que se desea redireccionar y después hacer click en ***Properties***.
4. En el cuadro ***Properties***, de la lengüeta ***Setting***, hacer click en una de las siguientes opciones:
   - ***Basic - Redirect everyone's folder to the same network share point.***
   Todas las carpetas afectadas por esta GPO se almacenan en la misma carpeta compartida de red.
   - ***Advanced - Redirect personal folders based on the user's membership in a Windows Server 2003 security group.***
   Las carpetas se redireccionan a otras compartidas de la red y basadas en los miembros de grupos de seguridad. Por ejemplo, carpetas que pertenecen a los usuarios del grupo de contabilidad se redireccionan al servidor de contabilidad, y
   las carpetas que pertenecen a los usuarios en el grupo de comercialización se redireccionan al servidor de comercialización.
5. En el cuadro ***Properties***, hacer Click en ***Add***.
6. Bajo ***Target folder location***, en el cuadro ***Root path***, ingresar el nombre de la carpeta compartida en la red a utilizar, o hacer click en ***Browse*** para localizarla.
7. En la lengüeta ***Settings***, configurar las opciones que se desean utilizar y después hacer click en ***OK***.

2.9. ¿Qué es Gpupdate?

```
gpupdate [/Target:{Computer | User}] [/Force]
[/Wait:Value] [/Logoff] [/Boot] [/Sync]
```

Gpupdate es una herramienta command-line que actualiza los local Group Policy settings y Group Policy settings almacenados en Active Directory, incluidas las configuraciones de seguridad. Por defecto, las configuraciones de seguridad se actualizan cada 90 minutos en un puesto de trabajo o un servidor, y cada cinco minutos en un Domain Controller. Usted puede correr gpupdate para probar una Group Policy setting o aplicar inmediatamente un Group Policy setting

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Los ejemplos siguientes demuestran cómo Usted puede utilizar el comando gpupdate:

```
C:\gpupdate
C:\gpupdate /target:computer
C:\gpupdate /force /wait:100
C:\gpupdate /boot
```

Gpupdate tiene los siguientes parámetros.

- ***/Target:{Computer | User}*** Especifica la actualización solamente de usuario o computadora para sus policy settings. Por defecto, la policy de usuario y computadora son actualizadas.

- ***/Force*** Reaplica todos los policy settings. Por defecto, solamente los policy settings que han cambiado se reaplican.

- ***/Wait:{Value}*** Fija el número de segundos para esperar el procesamiento de policy. Por defecto, es de 600 segundos. El valor ' 0 ' significa no esperar. El valor ' - 1 ' significa esperar indefinidamente.

- ***/Logoff*** Causa un logoff después de actualizar la configuración de Group Policy settings.

- ***/Boot*** Provoca que la computadora se reinicie después de la actualización de Group Policy settings.

- ***/Sync*** Provoca que la próxima configuración de policy setting se aplique sincrónicamente.

2.10. ¿Qué es Gpresult?

```
gpresult [/s Computer [/u Domain\User /p Password]]
[/user TargetUserName] [/scope {user|computer}] [/v]
[/z]
```

Debido a que Usted puede aplicar niveles traslapados de policy settings a cualquier computadora o usuario, Group Policy genera un reporte que resulta de aplicar policies al logon. ***Gpresult*** exhibe el reporte que resulta de aplicar policies que se hacen cumplir en la computadora para el usuario especificado al logon.

El comando ***gpresult*** exhibe los Group Policy settings y el Resultant Set of Policy (RSoP) para un usuario o una computadora. Usted puede utilizar ***gpresult*** para ver qué configuraciones de la GPO son efectivas y localizar problemas en la aplicación.

Los ejemplos siguientes demuestran cómo se puede utilizar el comando gpresult:

```
C:\gpresult /user targetusername /scope computer
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /scope USER
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /z >policy.txt
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23
```

Gpresult tiene los siguientes parámetros.

- ***/s Computer*** Especifica el nombre o dirección IP de una computadora remota. Por defecto es la computadora local.

- ***/u Domain/User*** El comando funciona con los permisos de la cuenta del usuario que se especifica User o Domain/User. El defecto son los permisos del usuario que se encuentre autenticado en la computadora y que ejecute el comando.

- ***/p Password*** Especifica el password de la cuenta del usuario que se especifica en el parámetro /u.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

- ***/user TargetUserName*** Especifica el nombre del usuario del que se exhiben los datos RSoP.

- ***/scope {user|computer}*** Exhibe los policy settings del usuario o computadora. Los valores válidos para el parámetro /scope son user o computer. Si se omite el parámetro /scope, gpresult exhibe a ambos, usuario y computadora.

- ***/v*** Especifica que la salida exhibirá información verbose de la policy.

- ***/z*** Especifica que la salida exhibirá toda la información disponible acerca de Group Policy. Dado que este parámetro produce más información que el parametro /v, se debe redireccionar la salida a un archivo de texto cuando se utilice este parámetro (por ejemplo, s puede escribir ***gpresult /z >policy.txt***).

- ***/?*** Exhibe la ayuda en la ventana de comandos.

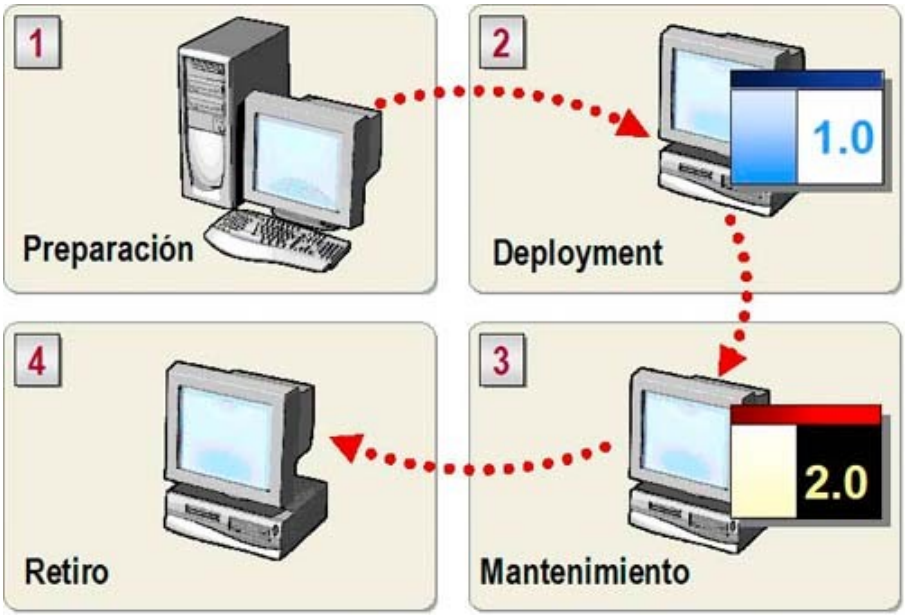
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3. Administración de instalación de Software

Microsoft® Windows® Server 2003 incluye una característica llamada Instalación y mantenimiento de software que utiliza el servicio de Active Directory®, Group Policy y Microsoft Windows Installer para instalar, mantener y quitar software en las computadoras en su organización. Usando el método de administración e instalación de software basado en policy, Usted puede asegurarse que los programas que los usuarios requirieran para realizar sus trabajos, estén disponibles siempre y donde sea necesario.

3.1. La instalación del Software y el proceso de mantenimiento



En Windows Server 2003, Usted puede utilizar Group Policy para manejar el proceso de instalación de software centralizado a partir de una localización. Además, Group Policy settings puede aplicarse a los usuarios o computadoras en un site, dominio u organizational unit para instalar automáticamente, actualizar o quitar software. Aplicando Group Policy settings al software, Usted puede manejar varias fases de la instalación del software sin instalar software en cada computadora individualmente.

La lista siguiente describe cada fase en la instalación del software y proceso de mantenimiento:

1. ***Preparation.*** Primero hay que instalar el software usanado la estructura corriente de Group Policy object (GPO), y también identificar los riesgos al usar la infraestructura actual para instalar software. Para preparar los archivos que permitan a un programa ser instalado con Group Policy, Usted debe copiar los archivos Windows Installer package para un programa a un software distribution point, el cual puede ser una carpeta compartida en un servidor. Asimismo puede adquirir el archivo Windows Installer package del vendedor del programa o crear el archivo package usando una utilidad de terceras partes.
2. ***Deployment.*** Aquí hay que crear una GPO que instala el software en la computadora y linkea la GPO a un contenedor apropiado de Active Directory. El software estará instalado cuando la computadora se encienda o cuando un usuario inicie el programa.
3. ***Maintenance.*** El software se actualiza con una nueva versión o reinstalando el software con un service pack o un software update. De esta maner, estará automáticamente actualizado o reinstalado cuando la computadora se encienda o cuando el usuario inicie el programa.
4. ***Removal.*** Para eliminar el software que no es requerido, se necesita quitar el software package setting de la GPO que originalmente instaló el software. El software entonces se quitará automáticamente cuando la computadora se encienda o cuando un usuario inicie sesion.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.2. ¿Qué es Windows Installer?

Para habilitar Group Policy para instalación y administración de software, Windows Server 2003 usa Windows Installer. Este componente automatiza la instalación y el retiro de programas, aplicando un sistema de reglas centralmente definidas durante el proceso de la instalación.

Windows Installer contiene dos componentes:

Windows Installer service. Este servicio del lado del cliente automatiza completamente la instalación del software y proceso de la configuración. El servicio Windows Installer puede también modificar o reparar un programa instalado existente. Para instalar un programa lo hace directamente del Cd-ROM o usando Group Policy. Para ello, el servicio Windows Installer requiere un Windows Installer package.

Windows Installer package. Este archivo package contiene toda la información que el Windows Installer service requiere para instalar o quitar software. El Archivo contiene:

- Un archivo Windows Installer con una extención .msi.
- Archivos fuente externos, que son requeridos para instalar o quitar el software.
- Información estándar sobre el software y el package.
- Archivos del producto o una referencia a un punto de instalación donde residen los archivos del producto.

Las ventajas de usar tecnologia Windows Installer incluye:

Custom installations. Características opcionales de un aplicativo. Por ejemplo, clip art o un diccionario, puede ser visible en un programa sin que la característica sea instalada. Aunque los comandos de menú son accesibles, la característica no está instalada hasta que el usuario acceda al menú de comandos. Este método de instalación ayuda a reducir la complejidad y la cantidad de espacio de disco duro que el programa utiliza.

Resilient applications. Si un archivo crítico se borra o se corrompe, el programa adquiere automáticamente una nueva copia del archivo de la fuente de la instalación, sin requerir la intervención del usuario.

Clean removal. Windows Installer quita aplicaciones sin dejar archivos huérfanos o inadvertidamente romper otro aplicativo, por ejemplo, cuando un usuario borra un archivo compartido que otro aplicativo requiera. También, Windows Installer quita todas las configuraciones de registry relacionadas y almacena las transacciones de instalación en una base de datos y archivos de log subsecuentes.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.3. Descripción del proceso de Software Deployment

Cuando Usted instala software, está especificando cómo se instalan los aplicativos y cómo se mantienen los mismos en su organización.

Para instalar nuevo Software, utilizando Group Policy, deberá:

1. ***Crear un software distribution point.*** Esta carpeta compartida en su servidor contiene el package y los archivos del software para instalar. Cuando el software se instala en una computadora local, el Windows Installer copia archivos a la computadora.
2. ***Utilizar la GPO para instalar software.*** Usted debe crear o realizar cambios necesarios a la GPO para el contenedor en donde desea instalar el aplicativo. Al mismo tiempo puede configurar la GPO para instalar software para una cuenta de usuario o de computadora. Esta tarea también incluye seleccionar el tipo de instalación que se requiere.
3. **Cambiar las características de la instalación del software.** Dependiendo de sus requisitos, Usted puede cambiar las características que fueron fijadas durante la instalación inicial del software.

3.4. Assigning Software vs. Publishing Software

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Los dos tipos de instalación son: asignar software y publicar software.

Usando la asignación de software, Usted se asegura que el software esté siempre disponible para el usuario. Cuando éste inicie sesión, aparecerán ***Start*** menu shortcuts y desktop icons para el aplicativo. Por ejemplo, si el usuario abre un archivo que utiliza Microsoft Excel en una computadora que no tiene Excel, pero Excel ha sido asignado al usuario, Windows Installer instala Excel en la computadora cuando el usuario abre archivo. Además, el asignar software hace al software resilient. Si por cualquier razón el usuario quita el software, Windows Installer lo reinstalará la próxima vez que el usuario inicie sesión e inicie el aplicativo.

Usando la publicación de software, Usted se asegura que el software esté disponible para que los usuarios lo instalen en sus computadoras. Windows Installer no agrega shortcuts en el escritorio del usuario o en el ***Start*** menu, y no realiza entradas en registry local. Dado que los usuarios deben instalar el published software, Usted puede publicar software solamente a los usuarios y no a las computadoras.

Usted puede asignar y publicar software usando uno de los métodos de la tabla siguiente:

Método de instalación	Método 1	Método 2
Asignación	Configurando al usuario. Cuando Usted asigne software a un usuario, el software se anunciará en el escritorio del mismo cuando inicie sesión. La instalación no comenzará hasta que el usuario haga doble-click al inicio de la aplicación o a un archivo asociado con la aplicación. Este es un método llamado activación de documento. Si el usuario no activa el aplicativo, el software no es instalado. De esta forma, se ahorra espacio en el disco duro y tiempo.	Configurando la computadora. Cuando Usted asigne software a una computadora, ningun aviso ocurrirá. En su lugar, el software se instalará automáticamente cuando la computadora se encienda. Asignando software a una computadora Usted se asegura que ciertos aplicativos estén siempre disponibles en esa computadora, sin importar quién la utiliza. Usted no puede asignar software a una computadora que sea domain controller.
Publicación	Usando Add or Remove Programs. Un usuario puede abrir el Control Panel y hacer doble-click en Add or Remove Programs para exhibir los aplicativos disponibles. El usuario puede seleccionar un aplicativo y entonces hacer click en Add.	Usando la activación de documentos. Si usted publica un aplicativo en Active Directory las extenciones de nombre de archivo de los documentos soportados por la aplicación serán asociadas en el directorio.

3.5. Práctica 7: ¿Cómo utilizar una GPO para instalar Software?

Después de crear un software distribution point, Usted deberá crear una GPO que instale esos aplicativos, y después linkear la GPO al contenedor que contenga los usuarios o computadoras en donde desee instalar el software.

Importante: No asignar ni publicar un Windows Installer package más de una vez en la misma GPO. Por ejemplo, si Usted asigna Microsoft Office XP a computadoras que son afectadas por una GPO, no deberá asignar ni publicar a los usuarios afectados por la misma GPO.

Para utilizar una GPO para instalar software, tendrá que realizar los siguientes pasos:

1. Crear o editar la GPO.
2. Bajo ***User Configuration*** o ***Computer Configuration*** (dependiendo si Usted está asignando el software a los usuarios o a las computadoras o publicándolo a los usuarios), expandir ***Software Settings***, hacer click derecho en ***Software Installation***, marcar ***New***, y después hacer click en ***Package***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

3. En el cuadro ***File Open***, hacer browse al software distribution point, usando el nombre Universal Naming Convention (UNC). Por ejemplo, **\\ServerName\ShareName**, seleccionar el archivo package y después hacer click en ***Open***.
4. En el cuadro ***Deploy Software***, seleccionar el método de instalación y después hacer click en ***OK***.

3.6. Práctica 8: ¿Cómo cambiar las opciones para la instalación de Software?

Un GPO puede contener varias configuraciones que afecten cómo un aplicativo es instalado, manejado y quitado. Usted puede definir las configuraciones por defecto global para los nuevos packages en la GPO, también puede cambiar algunas de estas configuraciones más adelante, editando las propiedades del package en la extensión de la instalación de software. Después de instalar un software package, recién podrá cambiar las características de la instalación que fueron fijadas durante la instalación inicial del software. Por ejemplo, Usted puede prevenir a usuarios la instalación del software package usando la activación de documento.

Para configurar las opciones implícitas para la instalación del software, deberá realizar los siguientes pasos:

1. Crear o editar la GPO.
2. Bajo ***User Configuration*** o ***Computer Configuration***, expandir ***Software Settings***, hacer click derecho en ***Software Installation*** y después en ***Properties***.
3. En la lengüeta ***General***, configurar las opciones siguientes de la instalación de software:

   - ***Default package location***
   - ***When adding new packages to user settings***
   - ***Installation user interface options***
4. En la lengüeta ***Advanced***, seleccionar la opción ***Uninstall the application when they fall out of the scope of management***.

Para cambiar las características de la instalación de software, deberá:

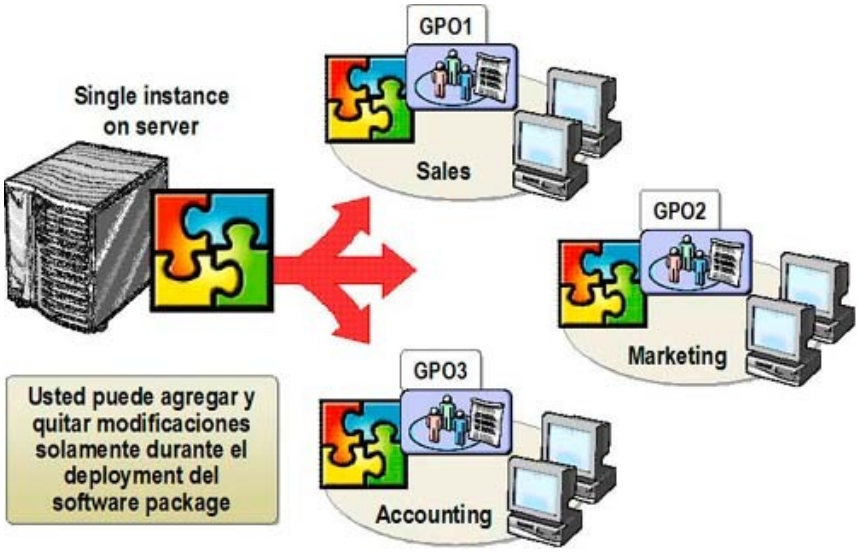
1. En Software Installation, hacer click derecho en el package instalado, y después hacer click en ***Properties***.
2. En el cuadro ***Properties*** de la lengüeta ***Deployment***, cambiar las siguientes opciones:

   - ***Deployment type***
   - ***Deployment options***
   - ***Installation user interface options***

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.7. ¿Qué es la modificación de Software?



Las modificaciones se asocian a un Windows Installer package en la instalación anterior que utilice ese Windows Installer package para instalar o modificar el aplicativo.

Instalar varias configuraciones de un aplicativo, permite a diversos grupos en su organización utilizar un paquete de software de diversas maneras. Usted puede utilizar modificaciones de software o archivos ***.mst*** (también llamado ***archivos de transformación***) para instalar varias configuraciones de un aplicativo. Un archivo .mst es un custom software package que modifica cómo Windows Installer instala el ***.msi*** package asociado.

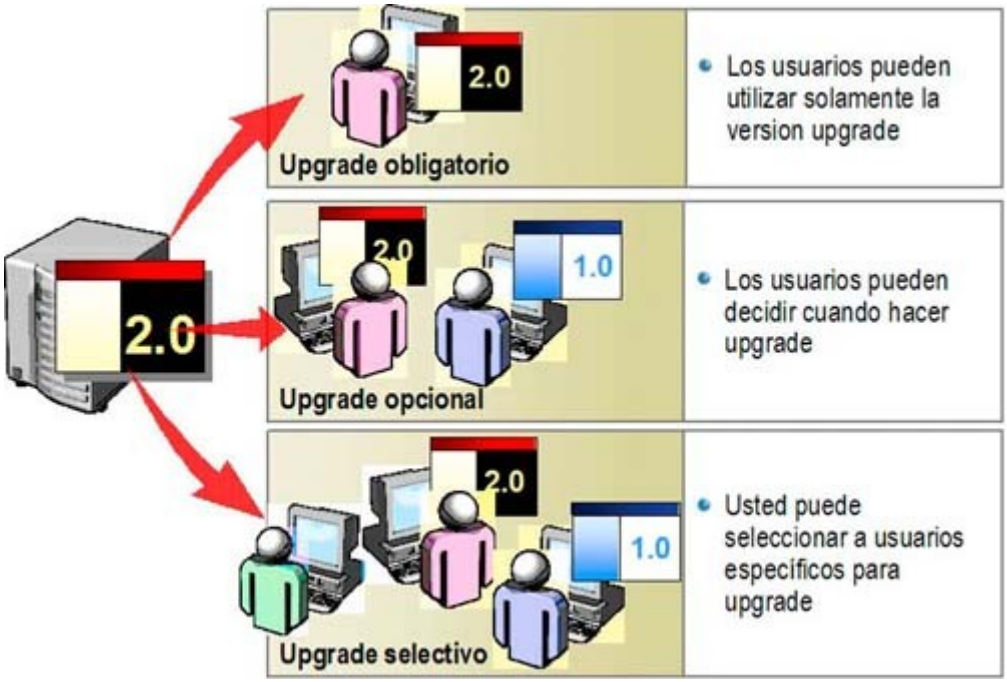
Windows Installer aplica modificaciones a packages en el orden que Usted especifique. Para guardar modificaciones en un archivo .mst, deberá correr el custom installation wizard y elegir el archivo .msi en el cual desea basar la transformación. Usted deberá determinar el orden en el cual aplicar las transformaciones a los archivos antes de asignar o publicar el aplicativo.

Ejemplo: Una organización grande, por ejemplo, puede querer instalar Microsoft Office XP, pero los requisitos por departamento para el Office suite varian extensamente en la organización. En lugar de configurar manualmente cada uno de los departamentos, Usted puede utilizar diferentes GPOs y archivos .mst en combinación con los archivos .msi por defecto, para que cada departamento instale varias configuraciones de Office XP. En este ejemplo, Usted puede correr el Office XP custom installation wizard del Office Resource Kit para crear el archivo de transformación.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.8. Tipos de actualización de Software



Las tareas en una organización son dinámicas y variadas. Usted puede utilizar Group Policy para instalar y administrar software upgrades que cumplan con requisitos departamentales en su organización. Las actualizaciones implican típicamente cambios importantes al software y tienen nuevos números de versión. Generalmente, un número substancial de archivos cambia para una actualización.

Varios acontecimientos en el ciclo de vida de un aplicativo pueden accionar la necesidad de una actualización, incluyendo lo siguiente:

- Una nueva versión del software se lanza y contiene nuevas y mejoradas características.
- Parches y seguridad o realces funcionales se han hecho al software desde el lanzamiento pasado.
- Una organización decide utilizar un software de diversos vendedores.

Hay tres tipos de actualizaciones:

Mandatory upgrades. Estas actualizaciones substituyen automáticamente una vieja versión del software con la nueva version. Por ejemplo, si los usuarios utilizan actualmente la versión del programa 1.0, se quita esta versión, y la versión del programa 2.0 se instala la próxima vez que la computadora se encienda o el usuario inicie sesión.

Optional upgrades. Estas actualizaciones permiten que los usuarios decidan cuándo actualizar la nueva versión. Por ejemplo, los usuarios pueden determinar si desean actualizar a la versión 2.0 del software o continuar usando la versión 1.0.

Selective upgrades. Si algunos usuarios requieren una actualizacion pero no otros, Usted puede crear GPOs múltiples para que se apliquen a los usuarios que requieran la actualización y crear los paquetes de software apropiados en ellas.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

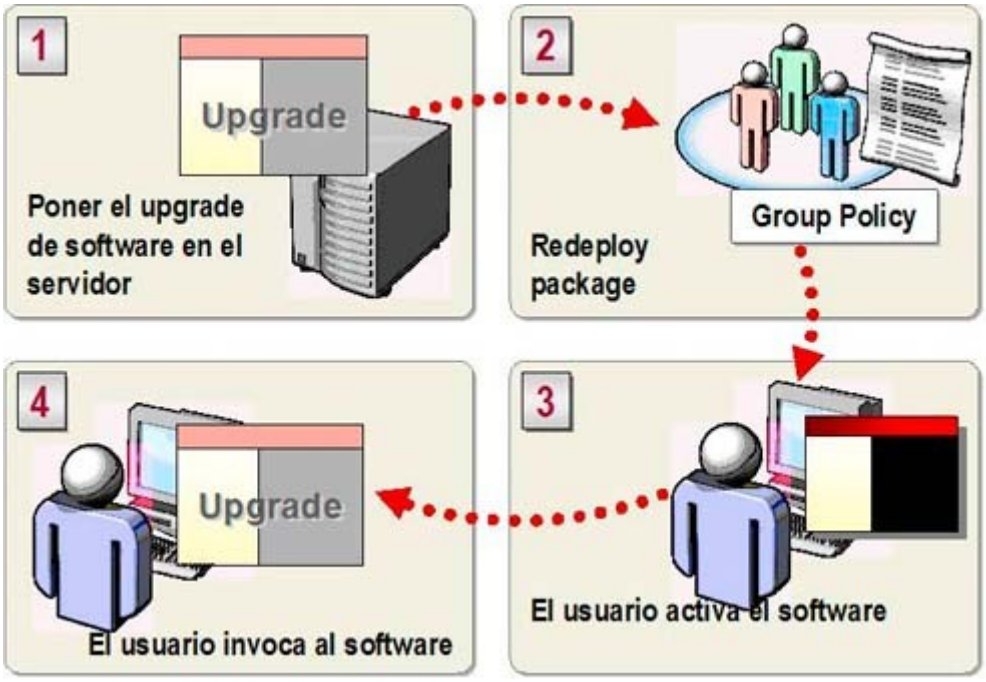
3.9. Práctica 9: ¿Cómo actualizar el Software instalado?

Usted utiliza la instalación de software para establecer el procedimiento de actualización de software a la versión actual.

Para instalar una actualización, deberá:

1. Instalar la versión siguiente del software.
2. Abrir Software Installation, hacer click derecho en la nueva versión, y después hacer click en ***Properties***.
3. En el cuadro ***Properties*** de la lengüeta ***Upgrades***, en la sección ***Packages that this package will upgrade***, hacer click en ***Add***, y despues seleccionar la versión anterior (actual) del software. Usted puede actualizar un aplicativo usando la GPO actual o seleccioando una GPO específica. Si ambas versiones del programa tienen un Windows Installer Package de forma nativa, este paso se realizará automáticamente.
4. Hacer Click en ***Package can upgrade over existing package o Uninstall the existing package, then install the upgrade package***, y despues hacer click en ***OK***.
5. Seleccionar el tipo de actualización:
   - Para realizar un mandatory upgrade, seleccionar el cuadro ***Required upgrade for existing packages***, y después hacer click en ***OK***.
   - Para realizar un optional upgrade, limpiar el cuadro ***Required upgrade for existing packages***, y después hacer click en ***OK***.

3.10. ¿Cómo funciona la reinstalación de Software?



Redeployment es la aplicación de service packs y actualizaciones de software al software instalado. Usted puede instalar un package instalado forzando la reinstalación del software. La reinstalación puede ser necesaria si el software package instalado previamente es actualizado pero sigue teniendo la misma versión, o si hay problemas de interoperabilidad o virus que la reinstalación del software arregle.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Cuando Usted marca un archivo package para reinstalación, el software se anuncia a cada uno de los que se ha concedido el acceso al aplicativo, ya sea a través asignación o publicación. Entonces, dependiendo de cómo el package original haya sido instalado, uno de estos tres escenarios ocurrirá:

- Cuando usted asigne software a un usuario, el ***Start*** menu, los shortcuts de escritorio y la configuración de registry serán relevantes al software y actualizados la próxima vez que el usuario inicie sesión. La próxima vez que el usuario inicie el software, el service pack o actualización de software se aplicará automáticamente.

- Cuando usted asigne software a una computadora, el service pack o actualización de software se aplicará automáticamente la próxima vez que la computadora se encienda.

- Cuando Usted publique e instale software, el ***Start*** menu, los shortcuts de escritorio y la configuración de registry, serán relevante al software y actualizados la próxima vez que el usuario inicie sesión. La próxima vez que el usuario inicie el software, el service pack o actualización de software se aplicará automáticamente.

3.11. Práctica 10: ¿Cómo reinstalar Software?

Usted utiliza la instalación de software para establecer el procedimiento de reinstalación del mismo. Antes de reinstalar, asegúrese que el servicio incluya un nuevo archivo Windows Installer package (.msi). De lo contrario, Usted no podrá reinstalar el software, porque solamente el nuevo archive package contiene las instrucciones para instalar los archivos nuevos que el service pack o actualización de software contiene.

Para reinstalar un software, deberá:

Obtener el service pack o actualización de software del vendedor del aplicativo y colocar los archivos en las carpetas apropiadas de instalación.

1. Editar la GPO que originalmente instaló el software.
2. Abrir Software Installation, hacer click derecho en el nombre del archive package, marcar ***All Tasks***, y después hacer click en ***Redeploy Application***.
3. En el cuadro de diálogo, hacer click en ***Yes***.

3.12. Métodos para quitar Software instalado

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Puede ser necesario quitar el software si una versión no es soportada en adelante o si los usuarios no requieren más el software. Usted puede forzar el retiro del software o dar a los usuarios la opción de continuar, usando el viejo software.

Hay dos métodos de remoción:

Forced removal. Usted puede forzar la remoción del software, lo cual automáticamente removerá el software de la computadora la próxima vez que la computadora se encienda o la próxima vez que un usuario inicie sesión, en caso de un Group Policy setting de usuario. El software se removerá antes que aparezca el escritorio del usuario.

Optional removal. Usted puede quitar el software de la instalación del mismo sin forzar el retiro físico del software. El software no se quita realmente de las computadoras. El software no aparece más en ***Add or Remove Programs***, pero los usuarios pueden todavía utilizarlo. Si los usuarios remueven manualmente el software, no podrán reinstalarlo.

3.13. Práctica 11: ¿Cómo quitar Software instalado?

Cuando Usted utiliza Group Policy para instalar software, puede configurar la GPO para remover el software viejo, si no es más requerido por su organización. También quitar software viejo configurando la GPO que permite a los usuarios un optionally upgrade a un nuevo software package.

Para quitar software instalado, deberá:

1. Abrir la GPO que fue utilizada originalmente para instalar el software.
2. En Software Installation, hacer click derecho al nombre del package, marcar ***All Tasks***, y después hacer click en ***Remove***.
3. En el cuadro ***Remove Software***, hacer click a una de las siguientes opciones, y después hacer click en ***OK***.

- ***Immediately uninstall the software from users and computers.***

- ***Allow users to continue to use the software, but prevent new installations.***

Nota: Usted debe asegurarse que los usuarios reinicien sus computadoras si el cambio afecta a la computadora, o que inicien sesión nuevamente si el cambio afecta al usuario.

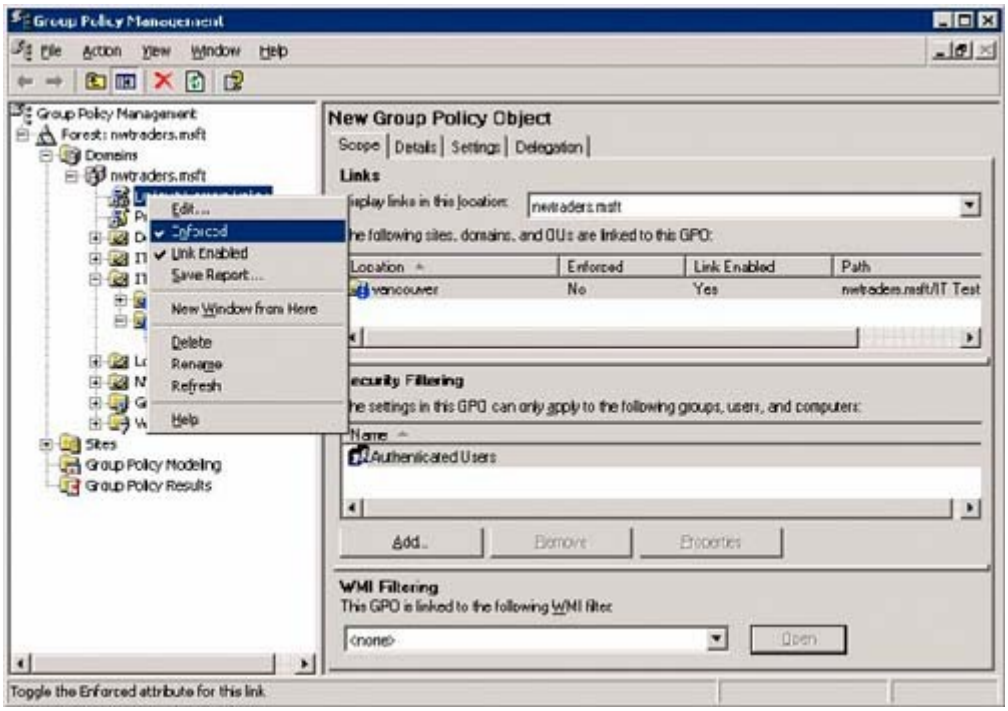
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

4. new! Group Policy Management Console (GPMC)

Conjuntamente con Microsoft® Windows Server. 2003, Microsoft está lanzando una nueva herramienta Group Policy Management que unifica la administracion de Group Policy. La Microsoft Group Policy Management Console (GPMC) proporciona una sola solución para manejar todas las areas relacionadas a Group Policy. Consiste en un nuevo Microsoft Management Console (MMC) snap-in y un sistema de interfases de scripting para la administración de Group Policy. La GPMC ayuda manejar una empresa con más eficacia.

4.1. ¿Qué es la Group Policy Management Console?



La Group Policy Management Console (GPMC) es una herramienta nueva para manejar Group Policy en Windows Server 2003.

La GPMC:

- Permite que usted maneje Group Policy para múltiples forests, dominios y organizational units a partir de una interfaz constante.
- Exhibe los links, herencia y delegación de Group Policy
- Muestra los contenedores a los cuales se aplican policy.
- Proporciona reportes HTML de las configuraciones.
- Proporciona las herramientas para mostrar el Resultant Set of Policies (RSoP) y experimentar con combinaciones propuestas de policies.

Nota: La GPMC no viene con Windows Server 2003. Usted puede descargarla de

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

4.2. GPMC Requisitos del Sistema

GPMC ayuda a manejar ambos dominios basados en Windows 2000 y Windows Server 2003 con Active Directory® service.

En cualquier caso, la computadora en la cual corre GPMC debe funcionar con uno de los sistemas operativos siguientes:

- Windows Server 2003.

- Windows XP Professional con Service Pack 1 (SP1) y Microsoft .NET Framework. Además, es requerido un hotfix post-SP1 (QFE Q326469). Este QFE actualiza su versión de gpedit.dll a version 5.1.2600.1186, la cual se requiere para GPMC. Este QFE se incluye con GPMC y la instalación de GPMC le pregunta sobre su instalación. Sin embargo, si el lenguaje de GPMC no concuerda con el lenguaje de su sistema operativo, GPMC no instalará el QFE y se necesitará obtener e instalar por separado este QFE, que será incluido en Windows XP Service Pack 2.

4.3. Instalación de GPMC

La instalación de GPMC es un proceso simple que implica la ejecución de un Windows Installer (.MSI) package. Los archivos necesarios serán instalados en la carpeta **\Program Files\GPMC**.

Para ello:

1. Hacer Doble-click en ***gpmc.msi*** package y en ***Next***.
2. Aceptar el End User License Agreement (EULA), y hacer click en ***Next***.
3. Hacer Click en ***Close*** para terminar la instalación.

Sobre la terminación de la instalación, la lengüeta Group Policy que aparecía en las páginas de propiedades de sites, dominios y organizational units (OUs) en el Active Directory snap-ins, es actualizada para proporcionar un acceso directo a la GPMC. La funcionalidad que existió previamente en la lengüeta original de Group Policy no estará más disponible; toda la funcionalidad para manejar Group Policy estará disponible a través de la GPMC.

Para abrir el GPMC snap-in directamente, utilizar alguno de los métodos siguientes:

- Hacer Click en ***Start***, click ***Run***, ingresar ***GPMC.msc***, y después hacer click en ***OK***.
- Hacer Click en el acceso ***Group Policy Management*** en la carpeta ***Administrative Tools*** del Start Menu o en el Control Panel.
- Crear una consola custom MMC

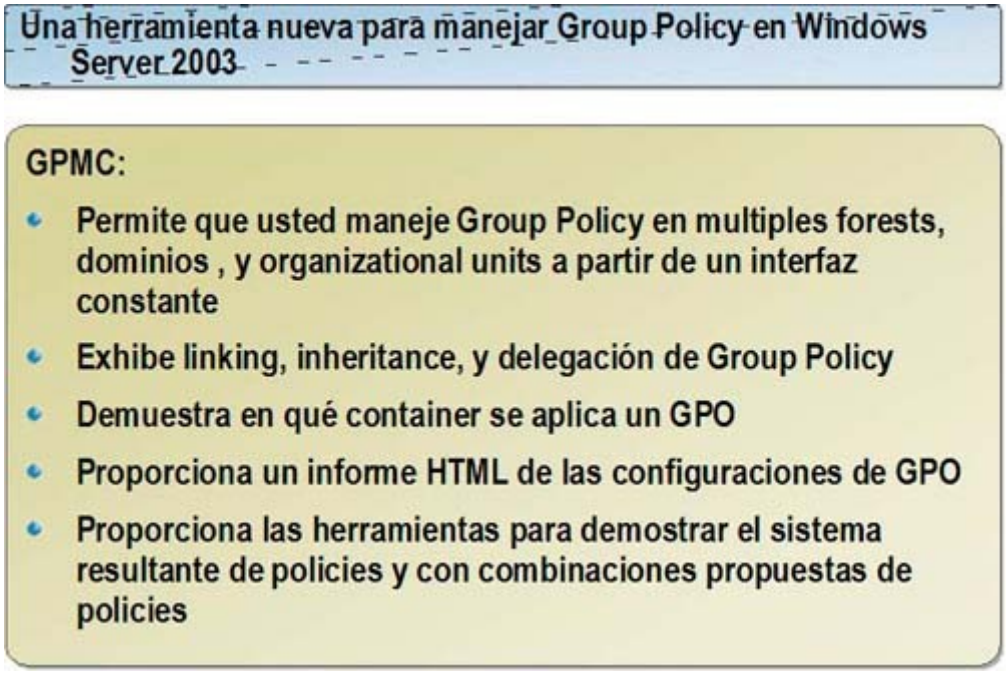
1. Hacer Click en ***Start***, click ***Run***, ingresar ***MMC***, y después hacer click en ***OK***.
2. En el menu ***File***, hacer click en ***Add/Remove Snap-in,*** hacer click en ***Add***, seleccionar ***Group Policy Management***, hacer click en ***Add***, hacer click en ***Close***, y después hacer click en ***OK***.

- Para reparar o quitar GPMC, usar ***Add or Remove Programs*** en Control Panel. Alternativamente, correr el gpmc.msi package, seleccionr la opción apropiada, y hacer click en ***Finish***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

4.4. Group Policy Modeling y Group Policy Results



Group Policy Modeling

Windows Server 2003 tiene una nueva característica de gran alcance: Group Policy Management. Esta permite que el usuario simule la aplicación de policy que sería aplicada a los usuarios y a las computadoras antes aplicar realmente policies. Esta característica, es conocida como Resultant Set of Policy (RSoP). El Modo de planeamiento en Windows Server 2003, se integra en GPMC como Group Policy Modeling. Esto requiere un domain controller Windows Server 2003 en el forest porque la simulación es realizada por un servicio que está solamente presente en domain controllers Windows Server 2003.

Sin embargo, usando esta característica, Usted puede simular el resultant set of policy para cualquier computadora en el forest, incluyendo las que funcionan con Microsoft Windows® 2000.

Group Policy Results

Esta característica permite que los administradores determinen el resultant set of policy que fue aplicada a una computadora específica y (opcionalmente) el usuario que inició sesión en esa computadora. Los datos que se presentan son similares a los datos de Group Policy Modeling. Sin embargo, son diferentes a Group Policy Modeling puesto que no son una simulación. Es el resultado real de resultant set of policy obtenido de la computadora destino. También difiere Group Policy Modeling, con los datos de Group Policy Results que se obtienen del cliente, y no se simula en el domain controller. El cliente debe correr Windows XP, Windows Server 2003 o superior. No es posible conseguir Group Policy Results para una computadora que corra Windows 2000 o anterior.

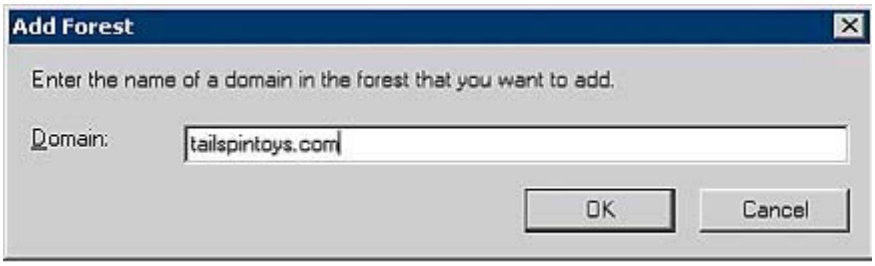
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

4.5. Administrando múltiples Forests

Múltiples forests pueden ser agregados fácilmente a la consola. Para ello deberá:

1. Hacer click derecho al nodo de la raíz ***Group Policy Management***, y seleccionar ***Add Forest...***



2. Especificar el nombre DNS o NetBIOS del dominio deseado en el forest que no se haya cargado en GPMC, y hacer click en ***OK***.

El forest especificado aparecerá como nodo secundario en la consola y será cargado en la consola con el dominio que fue incorporado en el cuadro ***Add Forest***.

Para quitar un nodo de forest, simplemente haga click derecho en el nodo, y seleccione ***Remove***. Por defecto usted puede agregar solamente forest a la GPMC si hay 2-way trust con el forest del usuario que corre la GPMC.

4.6. Contenido de Dominios

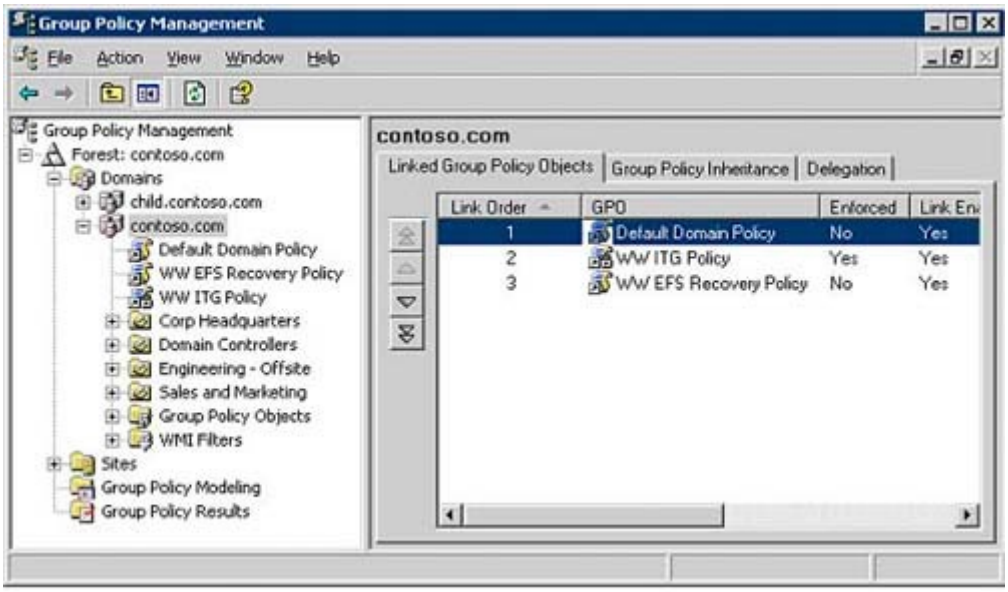
Dentro de cada dominio, GPMC proporciona una vista basada en policy de Active Directory y los componentes asociados a las Group Policy, por ejemplo, GPOs, WMI filters y GPO links. La visión en GPMC es similar a la visión en Active Directory Users and Computers MMC snap-in, que muestra la jerarquía de OU. Sin embargo, GPMC difiere de este snap-in porque en vez de mostrar usuarios, computadoras y grupos en OUs, exhibe las GPOs que están linkeadas a cada contnedor.

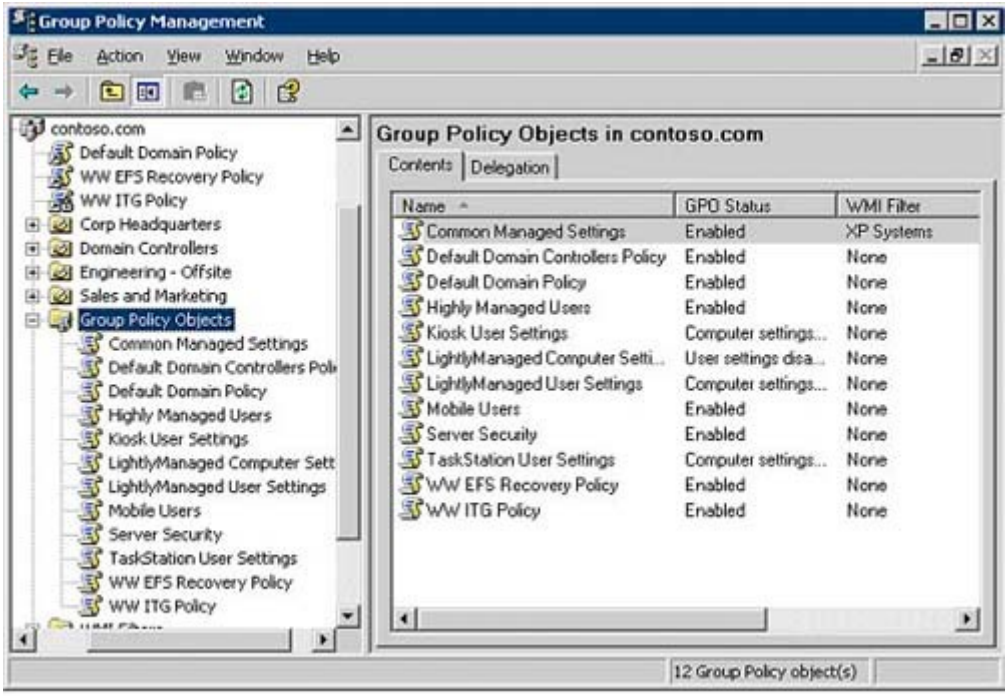
Cada nodo de dominio en GPMC exhibe los puntos siguientes:

- Todas las GPOs linkeadas al dominio.
- Todas las top-level OUs y una vista del árbol de OUs y GPOs linkeadas a cada una de las OUs.
- Los contenedores de ***Group Policy Objects*** muestran todas las GPOs en el dominio.
- El contenedor ***WMI Filters*** muestra todos los WMI Filters en el dominio.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by





4.7. Reportes de configuración de GPO

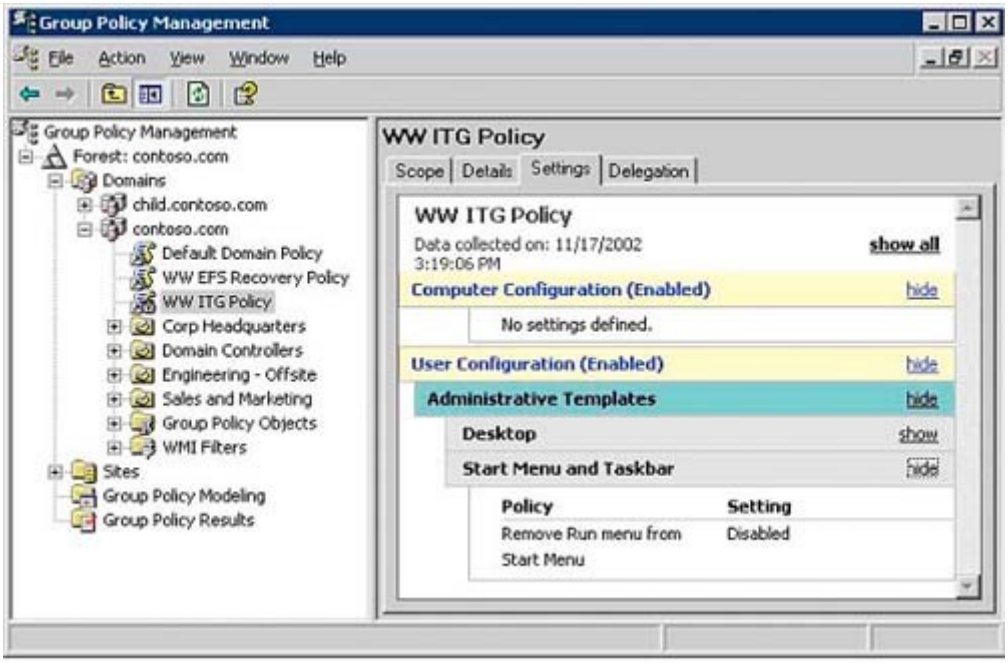
La lengüeta de configuración de GPO o GPO link en GPMC, muestra un informe HTML que exhibe todas las configuraciones definidas en la GPO. Haciendo click en esta lengüeta se genera un informe de las configuraciones en la GPO. Este informe puede ser generado por cualquier usuario con acceso de lectura al GPO. Sin GPMC, usuarios que no tenían acceso de escritura a un GPO no podrán leer y revisar configuracion en esa GPO. Esto es porque el editor de Group Policy Object requiere que el usuario tenga permisos de lectura y escritura al abrir la GPO.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Los informes HTML también hacen fácil que el administrador tenga visión de todas las configuraciones que se contengan en un GPO de un vistazo. Seleccionando la opción ***Show All*** arriba del informe, éste se amplía completamente y se muestran todas las configuraciones.

Para ver o guardar un informe directamente en un browser Web, Usted debe utilizar Internet Explorer 6 o Netscape 7. Netscape 7 no soporta la funcionalidad que permita mostrar u ocultar datos en informes.



4.8. Operaciones con GPO

Las operaciones GPO se refieren a la capacidad de ***backup*** (export), ***restore***, ***import*** y copy de GPOs. Hacer backup de GPO consiste en hacer copia de los datos de GPO al sistema de archivos. Observar que la función ***Backup*** también sirve como la función de la exportación para GPOs.

El Restore de GPO toma un backup existente y recrea la GPO en el dominio. El propósito del restore es reajustar un GPO específico de nuevo al estado idéntico que tenia cuando era realizado el backup. Por lo tanto, la operacion de restore no puede ser utilizada para transferir GPOs a través de dominios. Para esta operación debe utilizar la importación de GPO ó la operación de copy.

4.8.1. Backup

El Backup de GPO pone una copia de todos los datos relevantes de GPO en una localización especificada del sistema de archivos. Los datos relevantes incluyen:

- El GPO GUID y dominio.
- Configuraciones GPO.
- La Discretionary Access Control List (DACL) de la GPO.
- Los WMI filter link.

La operación de backup solamente hace backup de componentes de la GPO que están en Active Directory y en la estructura de archivo de GPO en SYSVOL. La operación no captura los datos almacenados fuera del GPO, por ejemplo WMI filters e IP Security policies. Éstos son objetos separados con su propio sistema de permisos y es posible que un administrador cualquiera que realiza el backup o el restore, pueda no tener los permisos requeridos en esos otros objetos.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

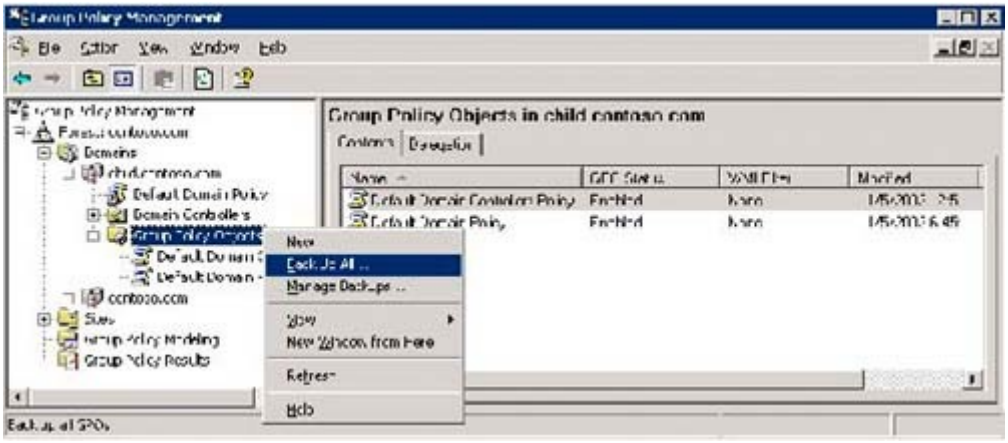
Los administradores pueden hacer backup de una o más GPOs usando los métodos siguientes:

- Hacer click derecho en la GPO bajo el nodo ***Group Policy objects*** y elegir ***Back up...*** del menú de contexto.

- Hacer click derecho en una o más GPOs en la lengüeta ***Contents*** del nodo ***Group Policy objects*** y elegir ***Back up...*** del menú de contexto. Esto hace backup de las GPO(s) seleccionadas.

- En el nodo ***Group Policy Objects***, hacer click derecho y elegir la opción ***Back Up All...*** Esto hace backup de todas las GPOs en el dominio.

- Use los GPO backup scripts. Usted puede escribir sus el propios scripts o puede utilizar la muestra de scripts incluida con GPMC en la carpeta GPMC\scripts . Hay dos scripts ***BackupGPO.wsf*** y ***BackupAllGPOs.wsf*** que se incluyen con GPMC, los cuales usted pueden utilizar para hacer backup de GPOs.



4.8.2. Restore

La operación de Restore de GPO restaura la GPO a un estado anterior y puede ser utilizada en los casos siguientes: se realiza backup a la GPO perose ha removido desde entonces, o la GPO está viva y se desea volverla a un estado anterior.

La operación de restore substituye los componentes siguientes de una GPO:

- Configuraciones de GPO.
- ACLs en la GPO.
- Los WMI filter links.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Usted puede realizar un restore de GPOs usando cualquiera de los métodos siguientes:

- Para hacer restore una GPO existente, hacer click derecho a la GPO en el contenedor ***Group Policy objects*** y seleccionar ***Restore from Backup...*** Esto abre el ***Restore Group Policy Object Wizard***.

- Usar los GPO restore scripts. Usted puede escribir sus propios scripts o utilizar las muestras de scripts incluídas con GPMC en la carpeta **GPMC\scripts**
Hay dos scripts ***RestoreGPO.wsf*** y ***RestoreAllGPOs.wsf***.

4.8.3. Import

La operación de importación transfiere configuración en una GPO existente de Active Directory, usando un backup de GPO en la localización del sistema de archivos como su fuente. Las operaciones de importación se pueden utilizar para transferir configuraciones a través de GPOs dentro del mismo dominio, a través de dominios en el mismo forest o en forest separados.

Las operaciones de importación son ideales para emigrar Group Policy a través de ambientes donde no hay confianza.

Las operaciones de importación se pueden realizar usando cualquiera de los métodos siguientes:

- Hacer click derecho en la GPO bajo el nodo Group Policy Objects y hacer click en Import Settings. Esto iniciará un wizard que lo guiará en el proceso de seleccionar el backup y opcionalmente especificando una tabla de migración si es apropiado.

- Usar cualquiera de los scripts ***ImportGPO.wsf*** o ***ImportAllGPOs.wsf*** que se incluyen con GPMC.

4.8.4. Copy

1. Una operación de copia transfiere configuraciones usando una GPO existente en Active Directory como la fuente y crea un GPO nueva como su destino.

2. Una operación de copia se puede utilizar para transferir configuraciones a un GPO nuevo cualquiera en el mismo dominio, en otros dominios, en el mismo forest o en forest separados. Puesto que una operación de copia utiliza un GPO existente en Active Directory como origen, la confianza se requiere entre el origen y los dominios de la destino.

Las operaciones de copia se pueden realizar usando cualquiera de los métodos siguientes:

- Hacer click derecho en la GPO origin, elegir la copy y hacer click derecho en el contenedor ***Group Policy Object***s del dominio deseado de destino. Elegir la opción paste.

- Usar drag and drop para arrastrar la GPO origin al contenedor ***Group Policy Objects*** en el dominio destino.

- Usar el script ***CopyGPO.wsf*** command-line que se incluye con GPMC.

Para obtener mas información:

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx
http://www.microsoft.com/windowsserver2003/gpmc/migrgpo.mspx

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

http://www.microsoft.com/grouppolicy
http://www.microsoft.com/technet/grouppolicy

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso